**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF TEXAS**
**WACO DIVISION**

| | | |
|---|---|---|
| **PACSEC3, LLC,** | ) | |
| **Plaintiff,** | ) | |
| | ) | **Civil Action No. 6:20-CV-00914-ADA** |
| **v.** | ) | |
| | ) | |
| **NETSCOUT SYSTEMS, INC.,** | ) | **JURY TRIAL DEMANDED** |
| **Defendant.** | ) | |

# PLAINTIFF'S REPLY CLAIM CONSTRUCTION BRIEF

## TABLE OF CONTENTS

## I. ADEQUATE STRUCTURE IS PROVIDED IN THE CLAIM LANGUAGE (and there is no reason to look further).

NetScout's brief ignores the language of the claims. While the Asserted Patents use the phrase "means for," there is adequate structure provided in the claims themselves to overcome the presumption that 112(f) applies. The Asserted Patents specify the structure in the claim and provide "means," or new ways of using the functionality of that structure to prevent packet flooding attacks. The "means" are not separate structure but rather ways of using the disclosed structure for packet defense:

Claim 1 of the '190 patent specifically claims the firewall (or router) as the structure performing the functions:

> 1. A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising: **at least one firewall, said firewall comprising**: hardware and software serving to control packet transmission ... means for classifying data packets **received at said firewall**; means for associating a maximum acceptable transmission rate with each class of data packet **received at said firewall**; means for **said firewall** ...; and whereby, **said firewall** can use said information ....[1]

Further, claim 1 of the '564 patent[2] specifically claims the firewall as the structure performing the functions:

> 1. A packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host computers, communication lines and transmitted data packets, said system comprising: **at least one firewall, said firewall comprising**: hardware and software ... serving to control packet transmission between said networks; means for classifying data packets **received at said firewall** related to the consumption of at least one resource; means for associating a maximum acceptable transmission rate with each class of data packet **received at said firewall**; means for limiting the transmission

[1] Doc. No. 1-1 at 7:40-8:10.
[2] All other Asserted Claims from the '564 patent depend from Claim 1.

rate **from the firewall** ....[3]

Likewise, each independent claim from the '497 patent, claims 1, 4, 7, 10, 13 and 16 each specify that a router (or firewall) is the structure for performing the various functions:

> 1. A packet flooding defense system for a network comprising a plurality of host computers, **routers**, communication lines and transmitted data packets, said system comprising: ... **via packet marks provided by routers leading to said host computer**; said path **comprising all routers** in said network ....[4]
>
> 4. A packet flooding defense system for a network comprising a plurality of host computers, **routers**, communication lines and transmitted data packets, said system comprising: ... **received at a router** ... **received at said router**; **means for said router**... **said packets came to said router via packet marks provided by routers** ...; **said path comprising all routers**... **and means in said router for said router** to use said information....[5]
>
> 7. A method of providing packet flooding defense for a network comprising a plurality of host computers, **routers**, communication lines and transmitted data packets, ... determining a path ... **via packet marks provided by routers** ...; said **path comprising all routers** ....[6]
>
> 10. A method of providing packet flooding defense for a network comprising ... **routers**... determining a path by which data packets arrive at **said router via packet marks provided by routers** ... said path comprising all **routers** in said network via which said packets are routed to said computer; classifying data packets **received at said router via packet marks provided by routers** ... **received at said router**....[7]
>
> 13. A packet flooding defense system for a network comprising ... **routers**, ... said system comprising: means for determining a path ... **via packet marks provided by routers** ...; said path comprising all **routers** ....[8]
>
> 16. A packet flooding defense system for a network comprising ... **routers**, ..., said system comprising: **means for a router to determine a path** ... via packet marks provided by **routers leading to said router**; said path comprising **all routers**...; and **means for said router** to allocate the transmission rate....[9]

Additionally, NetScout completely fails to respond to PacSec3's explanation that, while adequate structure is disclosed for one of ordinary skill in the art, the Asserted Patent's

[3] Doc. No. 1-2 at 6:26-46.
[4] Doc. No. 1-3 at 8:9-27.
[5] Doc. No. 1-3 at 8:61-9:10.
[6] Doc. No. 1-3 at 9:45-61.
[7] Doc. No. 1-3 at 10:25-42.
[8] Doc. No. 1-3 at 11:7-23.
[9] Doc. No. 1-3 at 12:3-19.

Specification do in fact provide flow chart embodiments or representations of algorithms for performing the various disclosed functions for either a firewall or router.

## II. LEVEL OF ORDINARY SKILL IN THE ART

There is not a substantial difference between PacSec3's POSITA[10] and NetScout's POSITA.[11] In fact, NetScout's requirement of a bachelor's degree with 2-3 experience is equivalent to PacSec3's master's degree, especially when viewed through the prism of computer science bachelor's degrees curricula offered in the 2000's. Therefore, PacSec3 respectfully request the Court adopts its definition of a POSITA.

## III. NETSCOUT'S OPENING BRIEF ESTABLISHES PACSEC3'S ARGUMENT THAT SUFFICIENT STRUCTURE IS DISCLOSED

### A. The File History of the '190 Patent Establishes the Understanding of a POSITA

NetScout's expert argues that the examiner for the '190 patent establishes the failure to disclose structure.[12] However, the cited position actually establishes that a POSITA would understand that data packets are classified by a variety of methods and the '190 patent's firewall (or router) is not limited to any specific method of classification. In fact, the examiner specifically states that the header of a packet contains certain path information,[13] thus obviating NetScout's entire argument that structure for classifying is not disclosed as a POSITA understands the structure of a packet inherently has a header that contains path information. This is not a case where a POSITA is adding structure, but rather where the structure of a packet is known by a POSITA to have a header that contains information, which information can be added or modified by a router (or firewall). Thus, NetScout's statement that "[i]t is clear" that how to classify data packets is not disclosed[14] ignores the very detailed description in the specification for classifying

[10] Doc. No. 28-1 at ¶13.
[11] Doc. No. 31 at 3-4.
[12] Doc. No. 31 at 9-10.
[13] Doc. No. 31 at ¶13.
[14] Doc. No. 31 at 10.

data packets. In all cases for the '190 patent and the '497 patent, the data packets are being classified by a router or firewall, as specifically, and repeatedly, stated in the specification.[15]

### B. Steps or Algorithms for Performing the Various Functions are Disclosed in the Figures with Reference to the Description

NetScout's repeated argument[16] that the Asserted Patents fail to disclose an algorithm is grossly inaccurate. The specification, with reference to the Figures details how the claim invention is performed in various embodiments, as testified to by PacSec3's claim construction expert when in response to the question:

> Dr. Swamy, in all three cases of the '190, the '564, and the '497, do those flow charts provide enough enablement for one of ordinary skill in the art, that POSITA you were talking about, to devise an algorithm or pseudocode for performing these various means as disclosed in your declaration?[17]

He said:

> I mean, it's my considered opinion that it -- that there is enough information here for a POSITA to practice the invention in using the options that the invention provides for them. And all the necessary structure is there in the diagrams, in the specifications, and within the four corners of each of these patents.[18]

Dr. Swamy was resolute in providing that the description and the figures provide algorithms for the various functions.[19] A further explanation of the disclosure is provided in Section V(F).

## IV. CORRECTIONS FOR STRUCTURE OF THE '564 PATENT

### 1. means for classifying data packets received at said firewall[20]

**For the '564 patent:[21]**

| Plaintiff's proposed construction | Defendant's proposed | By:[22] |
|---|---|---|

[15] Doc. No. 1-1 at 5:67-6:6; 6:7-8; 6:16-18; 6:30-31; 6:40-47; 6:59-7:3; 7:8-22; 7:29-34.
[16] Doc. No. 31 at 9, 11, 13, 16, 17, 18, 18, 19, 22, 23, 24, 25, 26, and 27.
[17] Ex. A, Deposition of Dr. Narayanaswamy at 174:3-8.
[18] Id. at 174:14-21.
[19] Id. at 170:13-20.
[20] Claim 1 of the '564 patent.
[21] By mistake, plaintiff listed only support from the '190 patent and not the '564 patent in its Opening brief but now adds support from the '564 patent.
[22] J=Joint; P=Plaintiff; D=Defendant

| | construction | |
|---|---|---|
| Function: identifying classes of the data packets that are received at said firewall<br>Structure: 3:18 to 3:20; 3:42 to 3:49; 4:46 to 4:50; 5:10 to 5:18; Figure 1 provides details | Indefinite | J |

**2. means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall[23]**

**For the '564 patent:[24]**

| **Plaintiff's proposed construction** | **Defendant's proposed construction** | **By:** |
|---|---|---|
| Function: associating a maximum threshold rate of transmission for each identified packet class through said firewall<br><br>Structure: 3:18 to 3:20; 3:42 to 3:49; 4:46 to 4:50; 5:10 to 5:31; Figure 1 provides details | Indefinite | J |

For each of these terms from the '564 patent, the first clause of the claim provides that it is a 'firewall' that is performing the specified functions,[25] thus the structure is specifically claimed and there is no reason to proceed further. NetScout's ramblings otherwise ignore the precise claim language, a cardinal sin in claim construction. It is the firewall (or router) that is performing the claimed functions.

Additionally, adequate disclosure of the structure of a firewall and router is also provided in the specification of the '564 patent. The specification describes how the firewall performs the various functions, such as classifying data packets at the firewall[26] and associating a maximum acceptable transmission rate with each class of data packet received at said firewall.[27] In each case, it is the firewall that is claimed as performing the function. Claim 1 of the '564 patent specifically claims hardware and software associated with the firewall, i.e., a router,[28] as routers

[23] Claim 1 of the '564 patent.
[24] By mistake, plaintiff listed only support from the '190 patent and not the '564 patent in its Opening brief but now adds support from the '564 patent.
[25] Doc. No. 1-2 at Claim 1, Column 6, line 31 ("6:31").
[26] Id. at 5:10-22.
[27] Id. at 5:10-24.
[28] Doc. No. 28-1 at ¶s26-28.

are known to control the transmission of data packets.[29]

The software on the firewall or router for performing the functions is explained through the algorithms disclosed in Figure 1 of the '564 patent which illustrates a packet transmission control system 10 for managing traffic 14 between at least two data networks 18, 22. The firewall 42 includes hardware and software providing a non-redundant connection 46 between the networks 18, 22 and serves to control packet transmission between the networks 18, 22. The algorithm discloses maximum transmission rates (one of 12, 9, 20, or 4) and an associated class of data packet 66.[30]

Figure 1 discloses an algorithm and diagram by flowchart for classifying data packets 38 received at the firewall 42 related to the consumption of at least one resource. The flowchart further shows associating a maximum acceptable transmission rate 62 with each class 66 of data packet 38 received at the firewall 42. The flowchart further shows the maximum transmission rate can be set as a limit on the transmission rate of packets across the firewall. When transmission rates 62 from the firewall 42 are so limited, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through the network connection.[] Moreover, a firewall inherently possesses the capability to inspect and label or mark (i.e., classify) data packets based on their properties. These properties would include available location information that accurately and reliably provides the firewall with the locations from which and through which attackers are sending packet flood attacks[] as would be understood by one of ordinary skill in the art and as is disclosed in the highly related '497 patent.[] Figure 2 is an embodiment of an algorithm whereby the data packets 38 within each class 66 are further subclassified by locations 78 within one of the networks 18 from which those data packets 38 originated, or from which they were forwarded to the firewall 42. Based upon this identification, the firewall 42 will thus limit the transmission rate for data packets 38 of each subclass 68 from locations 78 within one of the networks 18 to provide locations 78 proportionally fair service of

[29] Id. at ¶15.
[30] Id. at ¶27.

forwarding data packets 38 to another of the networks 22. This algorithm supports further subclassification of data packets by location within a network from which they originated or were forwarded to the firewall. No location will be allocated more than its fair share of forwarding service. The patents cited in the prior art of this specification, US6154775 and US6304975, both show that firewalls are well-known in the prior art to have the ability to inspect and classify packets by their properties. In this invention, such classification would also include inspecting the data packets to discern the location information added to those packets by cooperating routers as disclosed in the highly relevant '497 patent. Using data packets that incorporate marks encoding the locations taken by the packet through a cooperating network of routers was not known in the art.[31]

## V. ARGUMENTS ADDRESSING NETSCOUT'S REMAINING COUNTERPOINTS

### A. Pacsec3 Agrees to Construe "Can Use" As "Uses" From Claim 1 of the '190 Patent

PacSec3 agrees with NetScout's proffered construction of "whereby, said firewall can use said information to allocate the transmission rate for each class in a desired way" as "whereby, said firewall uses said information to allocate the transmission rate for each class in a desired way."[32]

### B. router[33]

NetScout's prosecution history argument does not limit the term router, rather it differentiates a router and a firewall. Thus, any modification of the plan and ordinary meaning would be no more than "router, which is not a firewall."

### C. host computer[34]

[31] Doc. No. 28-1 at ¶28.
[32] From Claim 1 of the '190 patent.
[33] Claim 1 of the '190 patent; Claims 1, 4, 7, 10, 13, and 16 of the '497 patent.
[34] Claim 1 of the '190 patent; Claim 1 of the '564 patent; Claims 1, 4, 7, 10, 13, and 16 of the '497 patent.

NetScout's prosecution argument does not limit the term host computer, rather it differentiates a host computer and a firewall. Thus, any modification of the plain and ordinary meaning would be no more than "host computer, which is not a firewall."

### D. PacSec3 Withdraws Claim 6 of the '564 Patent[35]

Plaintiff withdraws its claims of infringement for Claim 6 of the '564 patent and thus obviates the need for any construction.

### E. PacSec3 Agrees the 'Whereby' Clause of Claim 2 of the '564 Patent is Limiting

The 'whereby clause of claim 2 of the '564 patent should be construed according to its plain and ordinary meaning. NetScout has not shown how any meaning other than the plain and ordinary meaning is necessary. Thus, the term should be construed as "whereby, said firewall will limit the transmission rate for data packets of each class from locations within one of said networks to provide proportionally fair forwarding service to other locations within said network that communicates through said non-redundant connection."[36]

### F. There is Adequate Disclosure of the Claimed Functions performed by the firewall and router.

#### 1. means for classifying data packets received at said firewall[37]

Descriptions of how the firewall or router classifies data packets is provided in the '190 patent (Doc. No. 1-1) at 5:38-53 and explained through flowchart embodiments of algorithms in Figures 1, 2, 3, 4, 5 and 6. Figure 7, Figure 8 and Figure 9 illustrate how a firewall protecting a network communicates the rate limit for packets routed to it or routed to it by class functions.

[35] Claim 6 of the '564 patent.
[36] Claim 2 of the '564 patent.
[37] Claim 1 of the '190 patent; Claim 1 of the '564 patent is handled above in Section IV.

**2. means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall[38]**

Descriptions of how the firewall or router associates a maximum acceptable transmission rate is provided in the '190 patent (Doc. No. 1-1) at 5:38-53 and explained through flowchart embodiments of algorithms in Figures 1, 2, 3, 4, 5 and 6. Figure 7, Figure 8 and Figure 9 illustrate how a firewall protecting a network communicates the rate limit for packets routed to it or routed to it by class functions.

**3. means for said firewall to find information for packets it receives regarding the path by which said packets came to Said firewall[39]**

The description provides that the computer can use the information, the maximum acceptable processing rate, to allocate the processing rate for each class (38) in a desired way among the places from which packets (30) are transmitted.[40] Figures 1-6 of the '190 and the '497 patent illustrate embodiments, or algorithms, in which path information associated with each packet can be combined with other properties to further sub-classify the packet and assign each distinct subclass a transmission rate.

**4. means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet[41]**

The software on the firewall or router for performing the functions is explained through the algorithms disclosed in Figure 1. The firewall 42 includes hardware and software providing a non-redundant connection 46 between the networks 18, 22 and serves to control packet transmission between the networks 18, 22. The embodiments of algorithms disclose maximum transmission rates (one of 12, 9, 20, or 4) and an associated class of data packet 66.[42]

---

[38] Claim 1 of the '190 patent; Claim 1 of the '564 patent is handled above in Section IV.
[39] Claim 1 of the '190 patent.
[40] Doc. No. 1-1 at 5:38-53.
[41] Claim 1 of the '564 patent.
[42] Doc. No. 1-2 at Figure 1.

**5. means for said firewall to measure the amount of service requested by each packet[43]**

Figure 3 portrays an embodiment of an algorithm for this claim term whereby the firewall 42 maintains a memory of recently forwarded data packets 90 and classifies arriving data packets 38 as either data packets 86 sent from one of the networks 18 in response to at least one of the recently forwarded data packets 38 from another of the networks 22 or data packets 94 not sent in response to any recently forwarded data packets 38. The firewall 42 will thus limit the transmission rate of data packets 94 that are not sent in response to any recently forwarded data packets 38. The flow chart and algorithm for this claim term is also disclosed in Figure 4 showing the firewall (or a computer associated with it) as containing the algorithm disclosed. Two exemplary services disclosed are "requests for file transfer to B" and "requests for web page retrieval from C."[44]

**6. means for said firewall to measure the amount of service consumed in order to send each identified response data packet[45]**

Figure 5 discloses a flowchart and an embodiment of an algorithm for a firewall for classifying data packets 38 received at the firewall 42 based on requests for service. Figure 5 further shows firewall 42 measures the amount of service 36 requested by each identified data packet 38.

**7. means for storing and recalling past measurements of amounts of service provided for each type of service[46]**

To the extent that the recitation of memory is not sufficient structure for means for storing, reference is made to Figure 6 for an embodiment of the algorithm.

**8. means for classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/...by path[47]**

---

[43] Claim 4 of the '564 patent.
[44] Doc. No. 1-2 at Figure 4 (also shown in Figures 5 and 6).
[45] Claim 5 of the '564 patent.
[46] Claim 6 of the '564 patent.
[47] Claims 1, 4, 13 and 16 of the '497 patent.

Due to the fact that the '190 and the '497 patent share a common specification, PacSec3 references its argument made in Section V(F)(1), fully incorporated herein.

**9. means for associating a maximum acceptable processing rate with each class of data packet received at said computer[48]**

Due to the fact that the '190 and the '497 patent share a common specification, PacSec3 references its argument made in Section V(F)(2), fully incorporated herein.

**10. means for said computer to find information for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer[49]**

Due to the fact that the '190 and the '497 patent share a common specification, PacSec3 references its argument made in Section V(F)(3), fully incorporated herein.

**11. means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate[50]**

Figure 1 discloses this function by flowchart and diagram.[51] Figures 2-6 illustrate additional embodiments, or algorithms, in which path information associated with each packet can be combined with other properties to classify the packet and assign it a processing rate.[52]

**12. means for said router to find information for packets it receives regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer[53]**

Figures 3, 6, and 9 of the '497 patent describe the operation, or embodiment of an algorithm, of the router in finding path information for packets received via packet marks.

**13. A router is disclosed as performing each of the claimed functions**

---

[48] Claim 1 of the '497 patent.
[49] Id.
[50] Id.
[51] Narayanaswamy Decl. at ¶57.
[52] Doc. No. 1-3 at Figures 2, 3, 4, 5, and 6.
[53] Claim 4 of the '497 patent.

**a. means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate[54]**

**b. means for determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer[55]**

**c. means for assigning a maximum acceptable processing rate to each class of data packet[56]**

**d. means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets[57]**

Figures 1-6 of the '497 patent describe, and disclose algorithms for, how a router 22 is capable of receiving information regarding maximum acceptable transmission rate 70 for each class 38 of data packet 30 being transmitted to the computer 18 and the router 22 is capable of controlling the rate of transmission of each class 38 of data packets 30 to the computer 18.[58] Figure 7, Figure 8 and Figure 9 illustrate how a firewall protecting a network communicates the rate limit for packets routed to it or routed to it by class functions.[59]

## VI. CONCLUSION

PacSec3 respectfully requests the Court adopt its constructions.

Respectfully submitted,

Ramey & Schwaller, LLP

---

[54] Id.
[55] Claim 13 of the '497 patent.
[56] Id.
[57] Id.
[58] *See* Doc. No. 1-3 at 6:46-51.
[59] Id. at Figures 7, 8, and 9.

William P. Ramey, III
Texas Bar No. 24027643
wramey@rameyfirm.com
5020 Montrose Blvd., Ste. 800
Houston, Texas 77006
(713)426-3923
(832)900-4941 (fax)

**CERTIFICATE OF SERVICE**

The undersigned certifies that the foregoing document was filed electronically in compliance with local rules and the rules of civil procedure. As such, this pleading was served on all counsel who have consented to electronic service on May 17, 2021.

William P. Ramey, III
William P. Ramey, III